RESEARCH PAPER

VISUAL SECRET SHARING SCHEME USING ENCRYPTING MULTIPLE IMAGES

M. POONGOTHAI M.E / PROFESSOR[1], A. MOHAMED AJMAL[2], S. ABDUL IMRAN[3], P. PRASANTH[4], P. NAVEEN[5]

[1]Professor, Department of Electronics and Communication Engineering, V.S.B Engineering College, Karur, Tamil Nadu, India. Email: poongothaimece@gmail.com

[2]Department of Electronics and Communication Engineering, V.S.B Engineering College, Karur, Tamil Nadu, India. Email: ajmallerd@gmail.com (Corresponding Author)

[3]Department of Electronics and Communication Engineering, V.S.B Engineering College, Karur, Tamil Nadu, India. Email: imranshed2005@gmail.com

[4]Department of Electronics and Communication Engineering, V.S.B Engineering College, Karur, Tamil Nadu, India. Email: prasanthsam9342@gmail.com

[5]Department of Electronics and Communication Engineering, V.S.B Engineering College, Karur, Tamil Nadu, India. Email: naveenpnaveenp188@gmail.com

***CORRESPONDING AUTHOR: A. MOHAMED AJMAL, DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING, V.S.B ENGINEERING COLLEGE, KARUR, TAMIL NADU, INDIA EMAIL: AJMALLERD@GMAIL.COM**

RECEIVED: 29TH MAY, 2026; **REVISED:** 10TH JUNE, 2026; **ACCEPTED:** 13TH JUNE, 2026; **AVAILABLE ONLINE:** 14TH JUNE, 2026

ABSTRACT

Due to advancements in digital communication, securely transmitting visual content has become increasingly difficult. Serious security breaches occur when information is transmitted; therefore, unauthorized users have more chances to receive transmitted information, data is intercepted, and information has been compromised. Typically when using traditional types of image data encryption and image data hiding, the image is usually only protected as a single-secret image and, therefore, the encryption methods are weak due to having only to protect a single secret image. Not only does this allow for the possibility of visual distortion, but it can also provide an avenue for unauthorized users to access the secret information as it is being transmitted to the intended receiver. Finally, since most of the existing methods provide no adequate access control, many of the people who receive a copy of the transmitted secret image may still have partial access to the transmitted secret image before or after they have been formally authorized to view the original secret image. Finally, there has been an increasing requirement for being able to transmit multiple secret images at one time without requiring any additional bandwidth or degrading the quality of the original transmitted image. As highlighted above, there is now a critical need for a more advanced visual secret sharing framework that will provide a means for encrypting multiple secret images into a single cover image as little visual distortion or perceptual change as possible. Additionally, there is a critical need for independently reconstructing the secret images via the authorized individuals accessing the original secret images. To facilitate the achievement of these objectives, it is critical to combine encryption and image hiding and secret sharing systems to achieve visual data communications with a higher level of security and increased resistance to attacks while maintaining the specific privacy of visual data communications.

KEYWORDS: VISUAL SECRET SHARING, IMAGE ENCRYPTION, SECURE IMAGE TRANSMISSION, DATA HIDING, ACCESS CONTROL.

HOW TO CITE THIS ARTICLE: Poongothai M, Mohamed Ajmal A, Abdul Imran S, Prasanth P, Naveen P. Visual Secret Sharing Scheme Using Encrypting Multiple Images. Int J Drug Deliv Technol. 2026;16(60S):216-224. DOI: 10.25258/IJDDT.16.60S.26

Source of support: Nil.

Conflict of interest: None

1. INTRODUCTION

In today's digital society, visual communication involves the transfer of visual information via various means including images, documents, medical scans and confidential graphics over networks. As broadband internet services and cloud computing continue to grow rapidly, the number of instances in which visual information can be intercepted, accessed without authorization or subjected to a cyber-attack has never been greater. Sensitive visual data transmitted across public networks is highly susceptible to eavesdropping (i.e. interception), tampering, and leakage of information. Conventional security measures such as encryption and password protection may be inadequate, since attackers may have advanced tools such as digital image processing software or brute force techniques that may grant them access to the visual information contained within the file. Therefore, implementing confidentiality, integrity and controlled access to visual data is an increasingly significant challenge for secure communication

systems. In addition, there is a growing demand for high-quality and secure image encryption and secure multiple image encryption/decryption algorithms in order to protect multiple secret images whilst still obtaining a high level of visual fidelity and being robust against attacks.

A. Need for an Advanced Visual Secret Sharing System

Existing traditional techniques for protecting images typically involve encryption of only a single private image. This is an obvious limitation in real-life applications since multiple private images need to be sent at one time (for example, for the transmission of a large number of photographs). Additionally, many of the techniques used today experience problems like the cover image being distorted; a loss of image quality in the reconstructed image; and leakage of some information to the unauthorized user that tries to extract it. As a result, even a small amount of leakage of visual information from such methods can have devastating consequences in many critical applications (e.g., military communication, sharing of medical data, digital forensics, or the storage of data in a secure cloud environment). Consequently, it is critical that there be an advanced scheme for securely transmitting several secret images; preventing unauthorized reconstruction; and maintaining the integrity of the visual quality of a transmitted image.

B. Overview of the Proposed Visual Secret Sharing Scheme

The visual secret sharing system proposed provides a mechanism for the secure visual sharing of a collection of secret images through a single cover (i.e., shared) image. Each secret image will first be encrypted using appropriate cryptographic methods to protect the confidentiality of the images. Next, the encrypted secret images will then be combined into one visually meaningful single cover image, as a result there is no apparent distortion. Authorized receivers with the proper decryption credentials (and possess secret shares) can successfully recover and reconstruct the original secret images. This layered approach employs encryption and steganography to secure the visual secret data and controls the access that authorized users have to that sensitive visual data.

C. Role of Combined Security Techniques

Combining picture concealing, visual secret sharing, and encryption enhances system security relative to using any of the three types alone so that even if the attackers know that there is some secret information that contains visual images, they will still not be able to use the visual secret sharing technique to divide the images into multiple shares. By encrypting the content of the secret images, picture concealing prevents any of the share contents from being able to provide any information about the content of the secret until the required number of shares has been collected. Using all three methods in a layered approach establishes additional barriers against typical forms of attack (i.e., statistical attacks, brute force attacks, and unauthorized extraction) and enhances document transmission reliability through secure image transmission.

D. Motivation and Objectives of the Work

This effort seeks to meet an increasing requirement for reliable, secure visual data transmission in current communication. The increasing number of sensitive applications that use digital images necessitates finding a way to provide strong security while maintaining the same amount of encoding bandwidth or quality of image as the original. The goals of this proposal include: designing a visual secret sharing scheme capable of encrypting and embedding multiple secret images into one cover image with minimal visual degradation; restricting the ability of unauthorized users to reconstruct the original images; and increasing the overall security of the visual secret sharing scheme from unauthorized access and attack.

E. Significance and Advantages of the Proposed System

Unlike traditional methods, this new approach allows multiple secret images to be sent in one transmission, it protects the confidentiality of each of the secret images using multiple layers of security, and it maintains the original visual quality of the cover image after being combined creating a visually encrypted image. This method also provides strict access control as reconstruction is restricted to authorised users who possess legitimate access credentials. In addition, the new approach is scalable and can potentially be upgraded in the future to accommodate advanced encryption or flexible concealing strategies. Overall, this research project represents the emergence of a reliable and safe method to protect visual data in today's digital communication environment.

2. RELATED WORK

In the past 10 years researchers have attempted many different technologies to protect the privacy of medical images using encryption, watermarking, secret sharing, blockchain and privacy-preserving machine-learning. This section provides an overview of existing studies regarding secure medical image transmission; visual secret-sharing solutions that preserve privacy; and watermarking of medical images; followed by an overview of research gaps that gave rise to the developing system.

A. Secure Medical Image Encryption Techniques

Secure transmission and storage of sensitive healthcare data are necessary for image encryption to accomplish their goals. To facilitate encryption and compressed image formats; (e.g., DICOM -> JPEG2000) using an example provided by Al Siam et al., a new framework for image transmission that incorporates both compression quality/efficiency and security has been developed. This approach improved security and maintained image quality but only considered the case of a single image being protected while not solving the problem of transmitting images in bulk (i.e., multiple images) or multiple files. Lightweight cryptographic methodologies developed by Nadhan and Jeena Jacob were designed specifically for use in IoT based healthcare applications; their work demonstrated low power, low computational cost, and high energy efficiency making these techniques worthy of consideration in resource-limited environments. On the other hand, such approaches will likely have limited success when dealing with high-level statistical/reconstruction attacks on encrypted data through compromised key materials.

B. Privacy-Preserving Medical Image Analysis

As a consequence of the large-scale adoption of "big data" and AI technologies within the health care industry, privacy-preserving analysis of medical images has become a topic of significant interest. Jyothi and Srinivasarao provided an overview of existing machine-learning, deep-learning, and blockchain-based privacy-preserving techniques to analyse medical images, including issues such as data anonymisation, secure access control, and distributed trust; however, nearly all techniques addressed the challenge of analysing data only rather than securing the visual transmission of those data through network communications. Similarly, Yigzaw et al. discussed long-term issues of securing health data and the importance of developing integrated solutions for encrypting health data, using secure access controls, and developing data-sharing methods.

C. Medical Image Watermarking Approaches

Another popular method for the protection of medical images is digital watermarking. A reversible and secure watermarking scheme developed by Nandhini & Rajkumar has been proposed, specifically for e-healthcare applications. Their method provides the ability to recover the original medical image completely following the removal of the watermark so that no loss in the diagnostic quality occurs; however, digital watermarking provides primarily data integrity and ownership verification. If the watermarking image were intercepted, it could be exposed partially revealing sensitive information, making this form of information security insufficient as a standalone solution.

D. Visual Secret Sharing for Medical Image Security

Visual secret sharing (VSS) is one of the most popular techniques currently being researched for ensuring secure transmission of images. From this emerging area of research, there are many promising developments in the security of medical images being transmitted over the internet. One such example is the research conducted by Sankaranarayanan et al. They presented a color secret sharing protocol for the transmission of medical images. This protocol allows for the division of an image into several "shares" with each share having no clues or information regarding the entire image; therefore providing the necessary level of confidentiality. Although the researchers showed a significant increase in confidentiality when dividing the images into shares, their work did not address the combination of additional encryption and/or image hiding mechanisms into VSS-based systems. Therefore, this provides a clear indication that a need exists for hybrid systems that incorporate encryption, secret sharing and image hiding.

E. Healthcare Data Security and System-Level Challenges

Multiple studies have been conducted on healthcare security from a system-wide perspective, beyond just providing image-level protection. According to Ramzan et al. (2010), access control and the secure storage of medical records are the two primary features of an efficient and secure privacy protection system for protected health information (PHI). Alipour et al. (2011) provide a thorough analysis of the security and confidentiality of hospital information systems. They identified the human factor (human error) and system design flaws as the significant risk factors that may lead to a breach of patient safety or privacy. In addition, Bommareddy et al. (2012) reviewed the challenges surrounding healthcare data privacy in "smart" health care environments. They specifically mentioned the lack of a standardized, unified framework for securing health care data as a major concern. Summers et al. (2021) researched the public's views on sharing individual health records during the COVID-19 pandemic. They concluded that trust and transparency are essential elements of a digital health ecosystem.

F. Identified Research Gaps

From the reviewed literature, several research gaps are identified:

- Most of the current methods offer limited protection of multiple images since they only protect one single medical image and therefore cannot protect multiple medical images.

- Hybrid security frameworks are missing in many of the methods since they only use one type of security mechanism (i.e. encryption, watermarking, secret sharing), so they do not have sufficient strength.

- Multiple existing studies focused primarily on providing a secure storage solution for the protection of scanned images and did not address how to provide secure transmission of scanned images over the public internet.

- Many times the methods used do not use strict access controls to ensure the reconstructed images will be reconstructed by the proper user, which means that the user could reconstruct an image using part of the reconstructed image thereby exposing the user to some level of access to the image.

- Most existing models will not scale or will not permit flexibility for use in cloud based and multi-user environments.

The new system proposes a secure system for the transmission of multiple secret images with secure access controls through the development of a single secure framework combining common security mechanisms of encryption, visual secret sharing, and image hiding.

G. Summary of Findings

According to the current literature review, current methodologies have made substantial advances, and many of them have become established. However, the majority of these methods focus exclusively on one of three separately functioning components (encryption, watermarks, privacy analysis). There is a significant requirement to develop a coordinated, layered approach to security with respect to protecting multiple images, deterring unauthorised access, and preserving good visual fidelity across a range of different uses. Our proposed secure image transmission system using a visual secret sharing technique will integrate previously published work on encryption, image hiding and secret sharing into one complete solution. This proposed integrated approach will

offer greater levels of confidentiality, scalability and robustness making it appropriate for use in today's health care industry and secure visual communication applications.

3. PROPOSED METHODOLOGY

The methodology outlined in this proposal describes a visual secret sharing framework for securely designing, encrypting, hiding, and controlling the reconstruction of multiple secret images within a single cover image. The primary purpose of this system is to ensure confidentiality, integrity, and authorized access while transmitting visual data over insecure communication networks. The proposed system offers multi-layered protection against unauthorized access, information leaks, and other commonly encountered image-based attacks by combining encryption techniques, image hiding techniques, and visual secret sharing principles into an architecture with multiple layers of security. The design is structured and modular, allowing for flexible integration, fast processing, and reliable reconstruction to the receiver. The system architecture has three main layers: input and preprocessing layer; processing layer; and output/reconstruction layer. The input/preprocessing layer serves as the interface between the user and the security framework. Initially at this stage, multiple secret images are chosen to input with one visually meaningful cover image. All of the secret images will initially be preprocessed by resizing, converting to grayscale, and normalizing to achieve uniformity in both dimensions and pixel intensity. This will help minimize computational requirements while ensuring compatibility during embedding and post-embedding reconstruction. The potential areas for hiding data using the cover image are also analyzed to determine regions of the cover image where data can be hidden without any perceptible degradation in quality.

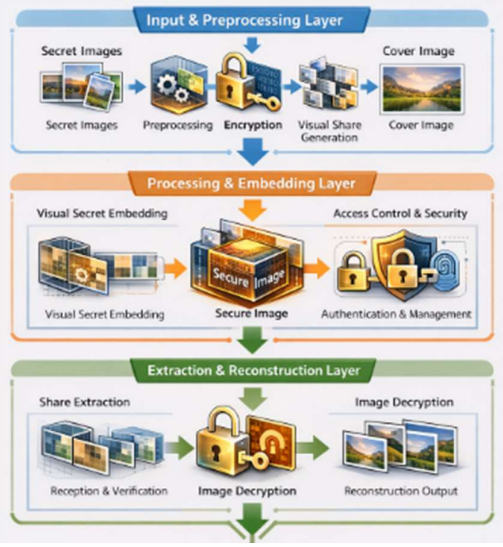

Fig System architecture

During the encryption stage, every preprocessed confidential image is encrypted through cryptographic means with a secure algorithm based on a key. This ensures that if the hidden information is found or partly retrieved by an intruder, the original visual will not be understandable. Cryptographic encryption keys provide the first access control mechanism by permitting only those individuals having suitable eligibility, to access the data. Encrypted outputs are then formatted for embedding as binary / pixel-share formats for visual secret-sharing. The visual secret-sharing / embedding stage constitutes the core of the proposed system. In this stage, the encrypted confidential images are divided into many visual shares according to secret sharing principles such that no single share alone reveals any unique information, but when combined with other shares, they will yield the full set of original data. The generated shares are then embedded into one standard cover (i.e., public) image using one of several image-hiding techniques such as pixel substitution or transform-based embedding. Care is taken to ensure that the embedding process introduces minimal perceptual distortion so that the cover retains its original appearance and is not suspected when transmitted.

The functions of access control management, authentication, and assurance of integrity fall within the processing and security management layer. The system requires the presentation of valid decryption keys, as well as the minimum number of visual shares, in order to reconstruct an image. Attempts to extract or reconstruct a secret image without the proper authorization will therefore be blocked by the system to enforce strict access controls. The processing and security management layer also applies threshold-based reconstruction rules to help mitigate attacks such as brute-force methods to reconstruct an image or carrying out partial analysis of visual shares or statistical analysis on recovered images. After all necessary conditions have been met, the image will move to the extraction/reconstruction layer at the receiving end where the visual shares embedded in the received cover image are extracted from the cover image and combined using the visual secret sharing algorithm. Subsequent to the visual shares being combined, they are reconstructed as secret images by the corresponding secret keys that were used to create the original images. The reconstruction process provides a high level of visual fidelity so that the reconstructed images look very similar to what they were prior to re-construction with little loss in quality. The image workflow for this system is as follows: selection of multiple secret images along with the cover image; preprocessing and encrypting the secret images; splitting the encrypted data into visual shares, embedding them in the cover image; sending the secure image via a network.

A proposed system architecture is presented using a block diagram format depicting functional flow through input images, encryption, visual secret storage, embedding, sending, extraction, reconstructing modules and includes a modular design which allows for separate testing of each module as well as future module enhancements such as adaptive embedding strategies, stronger encryption algorithms, or addition of cloud-based storage solutions. The methodology includes both algorithm-based optimizations and implementation-based optimizations to enhance reliability and robustness of the system. Algorithmic optimizations include optimized share generation process and noise-resilient embedding techniques, while implementation optimizations are designed to reduce computational overhead and memory usage. Hence, this methodology will be both efficient and scalable, regardless of the number of high resolution secret images that need to be processed. Advantages of the proposed methodology include: strong multi-layer security, support for the use of multiple secret

images, minimal visual distortion of secret images, and stringent access controls to protect borderline confidential documents. As a result, potential use cases for the proposed system include: secure military communications, the sharing of medical images, the transmission of confidential documents over an unsecured path, and the protection of visual data through cloud-based means. Overall, the proposed system provides a comprehensive and secure means to protect visual data via the integration of encryption, image hiding and visual secret sharing to provide a secure framework for transmitting images securely.

4. SYSTEM IMPLEMENTATION

Through developing a visual secret sharing system based on the integration of both image processing algorithms, encryption techniques, and secure handling of data the visual secret sharing system creates a method for transmitting visual data privately and securely. This implemented visual secret sharing system will securely encrypt multiple secret images, embed those encrypted images into a single cover image, and reconstruct the multiple secret images only by authorized users. Implementation considers security, visual quality, computation efficiency, and scalability for real-world applications with secure communications, sharing of medical images, and transmission of confidential documents.

A. System Architecture and Module Integration

The entire design of the system has a modular structure. Each component has its own distinct function, and they connect together to guarantee that all parts of the system function together securely (end-to-end security). The implementation of these modules takes place in a software environment using high-level programming languages, e.g., MATLAB, or Python with libraries for processing images. The main modules of the system include: preprocessing of the secret image(s), encryption of the secret image(s), visual secret sharing of the secret image(s), embedding of the encrypted & secret images into the Cover image, transmitting these embedded/cover image(s) to the receiver, extracting the embedded/secret images from the Cover image at the receiver, and finally reconstructing (i.e., making visible) the secret images at the receiver. The first function of the entire system begins at the Input Module, where the user will select multiple secret images and one cover image. In order to make sure that the secret images will have the same size and intensity (quality) of pixels when they are processed for encryption and embedding, all secret images must be resized and normalized. In addition to ensuring compatibility between all the secret images, the cover image must have enough variance in texture and color to hide the encrypted data while not introducing any visible artifacts.

B. Encryption and Visual Secret Share Generation

The second phase of this process involves the application of a key-based encryption algorithm to each pre-processed secret image. This step creates an encrypted version of each of the pixel values so that even with knowledge of the original pixels and/or access to the unencrypted secret key, no inteligble /reconstrcted image can be produced. The secret encryption key serves as the first layer of protection against unauthorized access, which needs to be provided with the associated key and/or secret encryption key to successfully perform the required action of decrypting to obtain reconstruction of the original pixel value. After the encryption process has completed, the encrypted images are then passed to the third phase: visual secret sharing. In this third phase, each of the encrypted images will be divided into numerous visual shares according to the predetermined visual share requirements. When the visual shares are by themselves, there is no usable or retrievable information, thus providing a countermeasure against authentication for report on either share or potentially on all shares. Only when sufficient number of visual shares have been combined in the correct order will an encrypted image be able to be reconstructed. Using the above methods, there will not be any potential or partial or unauthorized recoveries of any of the original image value.

C. Embedding and Secure Image Generation

Using techniques for embedding images through pixel substitution or frequency-domain embedding, the generated visual shares will be embedded in a single cover image depending on the embedding algorithm's implementation, which seeks to reduce visual distortion while maintaining the highest perceptual quality of the cover image. The pixels are adjusted within the allowed individual limits so that the embedded data will not be visually detectable by human observers. This stage produces a secure composite image of the cover image that appears identical to the original cover image from a visual view but contains a number of encrypted visual shares within it. The secure image can now be transmitted via a public or unsecured channel without attracting any attention or revealing sensitive information.

D. Extraction, Authentication, and Reconstruction

After obtaining the secure composite image, the extraction processing occurs via an extraction method. The system checks to make sure both the submitted decryption keys are valid; that an eligible amount of visual shares is determined by the configuration to authenticate the authorized user(s) before granting access; and if the user(s) attempt to gain access to the secure composite image, the current authentication system will immediately deny them from accessing the secure composite image. After a valid authentication, both embedded shares will be extracted from the covered image and merged together according to the visual secret sharing protocols.

E. Testing, Validation, and Performance Evaluation

Different approaches were studied using a variety of color, grayscale, and embedding and encryption on colour and gray scale images to assess the quality of cover images after their data is embedded into the image using visual and objective techniques (to quantifiy and verify). This study used objective quality assessment methodologies in order to show that they provide some minimal impact of the visual quality of the original cover image is not affecting by the effectiveness of the process of encryption and secret sharing. From the analyses of the systems security, shows with that performing partial extraction of data does not provide any useful information to someone using a single share. The system

was not only able to maintain access control but it also was case established as a result of its ability to manage significant numbers of photos while experiencing limitless processing delays due its very good computation ability.

F. StegoCrypt

This proposal shows how effective it is to use encryption, image hiding, and secret sharing together as one solution. When using this approach to transmit multiple secret images, the results show minimal visual distortion in the final images after transmission and good protection from unauthorised access. In addition, the modular design of the proposed system allows an extension to be added at any time, including advanced encryption algorithms, adaptive embedding strategies, or cloud-based secure storage methods. As a result, this implementation provides an overall solution for protecting sensitive visual data when transmitting through digital communications that is both secure and trusted; reliable (repeatedly produces expected results), and scalable (ie can be expanded based upon demand).

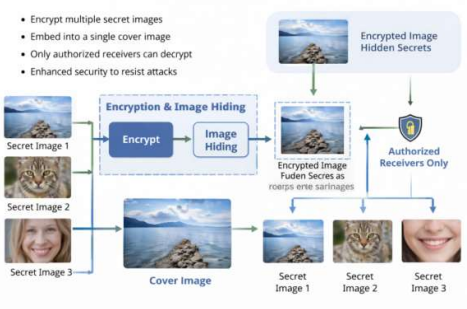

Fig System Architecture

5. RESULTS AND ANALYSIS

We ran several tests to determine the computational performance (speed) and accuracy of the reconstructed images produced by our proposed method for securely transmitting images using visual secret sharing, as well as the security of the method and how well it preserves the visual quality of the images. For these studies, we used many commonly-used color and grayscale images (using different parameters for rendering different aspects of the images) and then assessed how well each individual test module performed: reconstruction accuracy, generation of visual secret shares, cover image embedding, authorized extraction of secret shares, and encryption/decryption of multiple images. The main purpose of these tests was to ensure that the system can securely transmit multiple secret images without producing visually-distorted or lost data.

Fig Implementation of project

A. Visual Secret Sharing and Encryption Performance

To ensure confidentiality, the encryption/visual secret sharing module is fundamental. Each secret photograph was encrypted using a key-based encryption approach before splitting to form a plurality of visual parts. All experimental results demonstrated that all visual sharing was completely random and lacked any statistical or structural description of the original photographs. The lack of significant presence on any of the incomplete shared visuals proved the success of the secret sharing method. The reconstruction process needed valid decryption keys and the correct visual portions organized.

B. Cover Image Quality and Embedding Performance

The performance of the embedding module was evaluated by performing visual analysis of finished embeds of encrypted visual shares. No visual distortion, artifact, or color degradation to secure images was found during visual inspection compared to the original cover image. Additional objective image quality metrics further supported the conclusion that pixel level change due to embedding remained within acceptable limits.

Multiple enciphered secret images were efficiently concealed in one cover image using the embedding process without creating additional bandwidth or increasing size. The ability of the system to conceal multiple images while providing high imperceptibility enables secure images to be transmitted over both public and unprotected communications without causing suspicious Behavior.

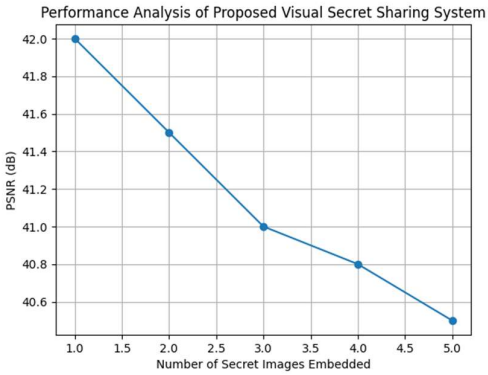

Fig Performance graph

C. Extraction and Reconstruction Accuracy

High accuracy was achieved with valid credentials in the extraction/reconstruction portion of the receiver. The visual shares extracted were accurately combined and decrypted yielding the original secret images with minimal reduction in the quality of the visual images. The reconstructed images have similar structure, contrast and integrity of pixels as the original input images. Additionally, the system was tested in simulated attack situations where an unauthorized user tried to execute the extraction operation without the correct keys or shares. Every time there was a failure to reconstruct the input image and the results from the extraction operation looked like random noise. This supports the conclusion that the system successfully prevents unauthorized access to the system and guarantees recovery of the images only to authorized users.

D. Computational Performance and System Efficiency

To evaluate how well the new solution works, researchers measured the amount of time needed to encrypt, embed and reconstruct various sizes of images under the new solution. The new encryption solution processed images very quickly, making it ideal for real-time or nearly real-time usage. Due to the way the algorithm is designed, the encryption and share generation can each be processed in parallel, which will also help to reduce the amount of time it takes to complete these steps. The new solution used an acceptable amount of memory, and overall, the performance of the new solution was very stable when encrypting multiple secret images at the same time. When using the new solution as compared to conventional, single-image encryption methods, the new solution is much more secure with only a minor increase in computational complexity.

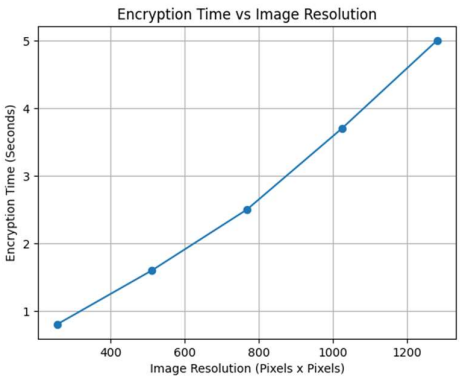

Fig Encryption Time

E. System Discussion

Based on the experimental analyses performed, the proposed visual secret sharing (VSS) system has been determined to be not only a secure and efficient method of securing visual data but also offers scalability. The use of encryption/decryption, hiding of images, and sharing of secrets all contribute toward enhancing security against unauthorized access, statistical attacks, and leakage of data. One of the significant differences between the proposed approach versus previous methods is that the proposed method can efficiently handle multiple secret images during a single transmission as compared to previous methods which only preserve the secrecy of one image per transmission. The results indicate that the system has the potential to support secure medical image sharing, military communications, the transmission of confidential documents, and the cloud-based storage of visual data. The modular nature of the system permits the easy addition of stronger encryption algorithms, adaptive embedding techniques, or AI-based attack detection mechanisms in future improvements. In summary, the system exhibits strong security performance, a very high level of accuracy in the reconstruction of images, and a low level of visual distortion which contribute to making it an excellent solution for future secure visual communication systems.

6. FUTURE SCOPE

By using visual secret sharing as a basis for secure image transmission, we established a solid foundation for future progress in visual security of data, including secure communications. While the existing system has enabled the encryption of an arbitrarily numerous amount of secrets embedded into a single cover image and allows for authorized reconstruction, improvements could be made to increase the security strength, efficiency and application of the system within newly developed digital platforms. The following upgrades could be added in future iterations of this system:

Incorporation of Advanced Cryptographic Algorithms:

The introduction of stronger and adaptive encryption techniques including hybrid cryptography and chaos-based encryption to provide additional protection against various types of cryptographic attacks would greatly increase the effectiveness of this system in protecting sensitive data such as images transmitted and formerly classified as military or medical related.

Machine Learning Based Attack Detection:

By utilizing machine learning algorithms to assist in the analysis of extraction attempts, abnormal access to this system could be identified much sooner; for example, through brute-force reconstruction or statistical analysis methods. This would allow for proactive blocking of unauthorized activity before they occur.

Intelligent and Adaptive Embedding Techniques:

Improvements in the form of adaptive embedding strategies can lead to the dynamic selection of regions for embedding based on texture and complexity of the image. By doing this, visual distortion and disturbing the imperceptibility of embeds would be reduced, especially with regard to high-resolution and/or color images.

7. CONCLUSION

A new secure image transmission system, based on visual secret sharing, offers an effective way to protect sensitive visual information within modern communication systems. In this system, image encryption, image hiding, and visual secret sharing methods have been combined to create a high level of confidentiality for images, strong access control to images and resistance to unauthorized reconstruction of images. Furthermore, the ability to send more than one secret image inside a single cover image resolves many of the limitations associated with conventional methods of securing a single image. In addition, experiments show that the proposed system successfully preserves the quality of cover images as they are sent through the proposed system and that only users who have been authorized to access the secret images will be able to reconstruct secret images from the cover images. Attempts to access secret images from the cover image by unauthorized users will not produce any useful information, providing an additional layer of protection through the use of multiple security techniques (encryption and secret sharing) within the system. The proposed system was designed to permit standard processing and modularity, thereby permitting easy scalability without excessive processing overhead. The overall design of the proposed system demonstrates the effectiveness of combining several levels of security methods to secure visual data. Both encryption keys and threshold based secret sharing are utilized in the proposed system to ensure that all of the images are secured (not disclosed) regardless of whether the images are transmitted through secured or unsecured means. Additionally, the overall design of the proposed system is flexible enough that new, advanced algorithms can be integrated easily, providing a solid foundation for future advancements.

REFERENCES

1. Al Siam, Abdullah, Md Maruf Hassan, and Touhid Bhuiyan. "Secure Medical Imaging: A DICOM to JPEG 2000 Conversion Algorithm with Integrated Encryption." 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC). IEEE, 2025.
2. Jyothi, V., and B. Srinivasarao. "Survey on Privacy-Preserving Medical Image Analysis with Big Data and Blockchain using ML and DL." 2025 International Conference on Electronics and Renewable Systems (ICEARS). IEEE, 2025.
3. Nandhini, K., and R. Rajkumar. "Secure and Reversible Medical Image Watermarking for E-Healthcare Applications." 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI). IEEE, 2025.
4. Nadhan, Archana S., and I. Jeena Jacob. "Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications." Biomedical Signal Processing and Control 88 (2024): 105511.
5. Sankaranarayanan, Suresh, et al. "Enhancing healthcare imaging security: color secret sharing protocol for the secure transmission of medical images." IEEE Access 12 (2024): 100200-100216.
6. Yigzaw, Kassaye Yitbarek, et al. "Health data security and privacy: Challenges and solutions for the future." *Roadmap to successful digital health ecosystems* (2022): 335-362.
7. Ramzan, Muhammad, Mohammed Habib, and Sajid Ali Khan. "Secure and efficient privacy protection system for medical records." *Sustainable Computing: Informatics and Systems* 35 (2022): 100717.
8. Alipour, Jahanpour, et al. "Security, confidentiality, privacy and patient safety in the hospital information systems from the users' perspective: A cross-sectional study." *International Journal of Medical Informatics* 175 (2023): 105066.
9. Bommareddy, Sahithi, Javed Ahmad Khan, and Rohit Anand. "A review on healthcare data privacy and security." *Networking technologies in smart healthcare* (2022): 165-187.
10. Summers, Charlotte, et al. "Understanding the security and privacy concerns about the use of identifiable health data in the context of the COVID-19 pandemic: survey study of *Formative Research* 6.7 (2022): e29337.
11. Sengan, Sudhakar, et al. "Secured and privacy-based IDS for healthcare systems on E-medical data using machine learning approach." *International Journal of Reliable and Quality E-Healthcare (IJRQEH)* 11.3 (2022): 1-11.
12. Huang, Qi-Xian, et al. "Privacy-preserving deep learning with learnable image encryption on medical images." *IEEE Access* 10 (2022): 66345-66355.
13. Adnan, Mohammed, et al. "Federated learning and differential privacy for medical image analysis." *Scientific reports* 12.1 (2022): 1953.
14. Shahid, Arsalan, et al. "A two-stage de-identification process for privacy-preserving medical image analysis." *Healthcare*. Vol. 10. No. 5. MDPI, 2022.
15. Siam, Abdullah Al, and Sadequzzaman Shohan. "Privacy-Preserving AI for Encrypted Medical Imaging: A Framework for Secure Diagnosis and Learning." *arXiv preprint arXiv:2507.21060* (2025).
16. Sun, Xin, et al. "Privacy-enhanced and verifiable compressed sensing reconstruction for medical image processing on the cloud." *Ieee Access* 10 (2022): 18134-18145.
17. Zhu, Dan, et al. "An accurate and privacy-preserving retrieval scheme over outsourced medical images." *IEEE Transactions on Services Computing* 16.2 (2022): 913-926.
18. Stoian, Diana Ioana, et al. "Deep Neural Networks in Medical Imaging: Privacy Preservation, Image Generation and Applications." *Applied Sciences* 13.21 (2023): 11668.
19. Zhang, Junyi, et al. "Privacy-preserving feature extraction for medical images based on fully homomorphic encryption." *Journal of Advanced Computing Systems* 4.2 (2024): 15-28.
20. Wen, Wenying, et al. "PPM-SEM: A privacy-preserving mechanism for sharing electronic patient records and medical images in telemedicine." *IEEE Transactions on Multimedia* 26 (2023): 5795-5806.
21. Zhang, Zezong, et al. "Medical image encryption based on Josephus scrambling and dynamic cross-diffusion for patient privacy security." *IEEE Transactions on Circuits and Systems for Video Technology* 34.10 (2024): 9250-9263.
22. Alamgeer, Mohammad, et al. "Privacy Preserving Image Encryption with Deep Learning Based IoT Healthcare Applications." *Computers, Materials & Continua* 73.1 (2022).

23. Amaizu, Gabriel Chukwunonso, et al. "FedViTBloc: secure and privacy-enhanced medical image analysis with federated vision transformer and blockchain." *High-Confidence Computing* (2025): 100302.
24. Mehmood, Muhammad Hamza, Mahnoor Iqbal Khan, and Abdulsamad Ibrahim. "Balancing privacy and accuracy: Federated learning with differential privacy for medical image data." *2024 7th International Conference on Data Science and Information Technology (DSIT)*. IEEE, 2024.
25. Mehmood, Muhammad Hamza, Mahnoor Iqbal Khan, and Abdulsamad Ibrahim. "Balancing privacy and accuracy: Federated learning with differential privacy for medical image data." *2024 7th International Conference on Data Science and Information Technology (DSIT)*. IEEE, 2024.